Influence Operations in Cyber: Characteristics and Insights

Deganit Paikowsky and Eviatar Matania[1]

Introduction

The reports on the attempts to influence the US presidential elections in 2016 through cyber activities bring to the forefront two different phenomena. The first is the expanding circle of targets threatened with cyberattacks: from the computerized systems of critical infrastructure that provide essential and tangible services to infrastructure, processes, and sectors that provide services that are less tangible but still essential to society and the state. For example, there is the possibility to penetrate computerized systems of national elections in order to change the voting results or to affect the concentration of the results, or to access the computerized systems of political parties, the media, polling companies, and even the public itself, in order to impair their functioning.

The second phenomenon is the use of the familiar type of influence operations while taking advantage of the unique characteristics of cyberspace.

[1] Dr. Deganit Paikowsky specializes in policy planning and strategy in the fields of science and technology. She lectures at the Security Studies graduate program at Tel Aviv University and previously served in a senior position at the Strategy and Capacity Building Division of the Israel National Cyber Directorate. Prof. Eviatar Matania is the founder and former Director of Israel's National Cyber Directorate. He currently serves as the director of the Security Studies program and a faculty member in the School of Political Science, Government, and International Affairs at Tel Aviv University.
This article does not represent an official opinion or strategy of the State of Israel or of the Israel National Cyber Directorate but is the personal analysis and opinion of the authors.

This is done by influencing, for example, the agenda, the perception of reality, and decision making during an election campaign in order to affect the results (without directly disrupting the elections process) and/or to sow doubt regarding the integrity and credibility of the elections and of the democratic process in general. For example, true, biased, or false information can be publicized with the aim of influencing and shifting public opinion, which is then expressed in voting patterns. Another method is to repeatedly disseminate certain messages on a massive scale via social media in order to shape the discourse in a certain direction.[2] It is important to note that when relevant target audiences (decision makers and/or the public) become aware of damage caused to the functioning of computerized systems, it may influence their cognition.

This article focuses on the overlap between cyberattacks and influence operations, or in other words, cyber actions whose aims are to directly affect cognition. While these influence operations are part of much wider cyber campaigns, they are also a component of the information wars, psychological operations, and attempts to influence decision makers through an entire array of information and narratives. Since the actions described here are located between cyberattacks and cognitive influence, they will be analyzed in parallel from both directions. Thus, a cyberattack that causes physical damage with the intention of paralyzing critical infrastructure, such as electricity or water, is not addressed in this article, even though it could also have cognitive side effects. However, if a cyberattack was carried out with the aim of causing panic or undermining public confidence in the system, then it should be considered having a direct cognitive effect. Similarly, a cyberattack whose goal is to change the election results by altering the data without being noticed is not a cognitive attack.

The phenomenon of cyber influence operations is gradually gaining appeal throughout the world and will likely become more common and elaborate. Therefore, it is necessary to understand the nature of the two phenomena detailed above – of which the cognitive influence via cyber is a part – by emphasizing their shared characteristics, but also, and perhaps especially, their unique features.

[2] David Siman-Tov, Gabi Siboni, and Gabrielle Arelle, "Cyber Threats to Democratic Processes," *Cyber, Intelligence, and Security* 1, no. 3 (2017): 51-63.

This article discusses the appeal of influence operations specifically in cyberspace and the differences between it and the familiar cyberattack. While the traditional cyberattack or cyber campaign seeks to cause tangible functional damage to the adversary, as its cognitive influence (if it even exists) is indirect, the purpose of influence operations is to harm the adversary by directly affecting cognition. Analyzing these two phenomena is especially critical for democratic states. In order to effectively prepare to defend against them, states must be aware that these are two different phenomena, despite having been placed together on the global agenda. Therefore, each one needs to be addressed differently.

Our main argument is that influence operations in cyberspace and through the use of cyber tools represent significant conceptual changes from the perspective of the cyber campaign; these operations rely on basic premises that differ from those in the familiar cyberattack, designed to impair the proper functioning of computerized systems. Effective defense against the threat of these operations requires an approach that considers the unique characteristics of this threat and its basic premises. Furthermore, it also demands comprehensive national preparedness and cooperation among a variety of bodies, of which cyber defense organizations are only a part.

The first part of the article analyzes the general characteristics of influence operations, including those in cyberspace. It also discusses the human and social characteristics upon which these operations are built. The second part focuses on the specific contribution of social media in making these operations appealing. The third part addresses the expanding targets of the cyber threats and specifically the similarities and differences between cyber actions designed to cause functional damage and those aimed at influencing cognition, which together constitute all cyber threats. The article concludes with initial insights that address the gaps identified in dealing with the challenges of the battle for cognition in cyberspace and the need to develop a comprehensive approach in order to effectively cope with influence operations.

A Strategy of Influencing Cognition

Influencing cognition is the ability to change and/or shape the conceptions of a person or a group of people, and as a result, to disrupt and/or change their behavior, decisions, and capabilities. This occurs by adding or removing topics within the public agenda and biasing the discourse on them.[3] Influencing cognition is based on a number of social and human characteristics. The first is human difficulty in distinguishing between true and false information, and in reconstructing what was true and false. The second characteristic is the inclination to take shortcuts in assessing the credibility of messages in the context of information overload. A third characteristic is the tendency of people to accept information that suits their worldview, even if it is false, and to accept and believe declarations and claims presumably supported by facts, even if they are false. For example, a display of objectivity strengthens the credibility of a propaganda statement when it is published on a news site.

An influence operation is an old, well-known method that aims to serve various political, military, economic, and social objectives. At the state level, influence operations seek to achieve their objectives by harming personal and economic security, undermining public confidence and support for state institutions, and damaging social solidarity. The means of achieving these objectives include actively intervening systems and processes, or using various kinds of leverage (economic and other) in order to prompt or prevent actions, and acquiring and using information in order to create and disseminate messages and cause them to reverberate so that they achieve the maximum effect. The channels for conveying messages are the traditional media (newspapers, radio, and television) as well as the new media; that is, the internet and its various applications, such as the social networks. Opinion leaders sometimes serve as "unaware agents" for strengthening the credibility of messages and widening their distribution.[4]

A strategy of influence operations is generally part of a holistic approach using multiple channels and means, sometimes referred to as "information warfare." This strategy aims to maneuver actors into behaving in a desired way, sometimes against their interests, in part, by distorting and influencing their picture of reality and exerting various kinds of leverage. These actions

[3] Karine Nahon and Shira Rivnai Bahir, "Election Propaganda in the Context of the Internet and Social Media: Background Information for the Beinisch Committee," January 2016 [in Hebrew].

[4] Ron Schleifer, "Psychological Warfare in Operation Cast Lead," *Maarachot* 43 (August 2010): 19-20 [in Hebrew].

are carried out toward decision makers and populations of adversaries and allies, during both peace and wartime.[5]

Recently, influence operations have intensified through the use of cyberspace. Cyberspace provides the foundations and the tools – both legitimate and illegitimate – to carry out these operations. To this end, information from computerized systems and databases is being used, even if only partly. According to reports from the US Director of National Intelligence (DNI), which assesses global threats, the United States considers influence operations, especially the cyber ones, to be a significant threat, whose scope, intensity, and importance are increasing.[6]

The Appeal of Influence Operations in Cyberspace and Social Media

The threat of cyber influence operations has intensified and increased as cyberspace, and especially the various social media applications, provide technological platforms and new tools to carry out these operations with unprecedented speed and power. Thanks to cyberspace, various targets for the purpose of gathering and disseminating information have become easily accessible, conveniently available, and fast, all at a relatively low cost.

[5] Dima Adamsky, "Cyber Operative Art: A Look from the Viewpoint of Strategic Studies and in Comparative Perspective," *Eshtonot* 11 (August 2015): 28-48 [in Hebrew].

[6] Daniel R. Coats, Director of National Intelligence, "Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community," Senate Select Committee on Intelligence, May 11, 2017; James, R. Clapper, Director of National Intelligence, "Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community," Senate Armed Services Committee, February 9, 2016; James, R. Clapper, Director of National Intelligence, "Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community," Senate Armed Services Committee, February 26, 2015; James, R. Clapper, Director of National Intelligence, "Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community," Senate Select Committee on Intelligence, January 29, 2014; James, R. Clapper, Director of National Intelligence, "Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community," Senate Select Committee on Intelligence, March 12, 2013; James, R. Clapper, Director of National Intelligence, "Statement for the Record – Worldwide Threat Assessment of the US Intelligence Community," Senate Select Committee on Intelligence, February 10, 2011.

From the attacker's perspective, conducting cyber influence operations is appealing because political achievements can be gained effectively and at a significantly lower cost than by using traditional tools (the most extreme being the use of military force). In addition, the ongoing paradigmatic change in how wars have been waged in recent decades has sometimes led to a preference for actions in cyber rather than on other levels, especially in terms of direct military conflict.[7]

Today, social media plays a central role in carrying out influence operations, serving as central "battlefields," as well as effective offensive channels for conducting influence operations.[8] There are several reasons for this. First, the number of people who use social media to consume information and directly interact at any place and time has grown exponentially in recent years.[9] In addition, the dissemination of information on social media occurs quickly within and between groups. Sometimes the spread of information happens so fast that it is difficult – if not impossible – to stop the process, known as the "virality of information flow."[10] The technological architecture of social networks, which aims to manage the flow of information by filtering excess information and exposing users to personalized information, is a significant component of the appeal of social networks as a platform for implementing influence operations.[11] The exposure of social media users only to a small portion of all the information on the internet helps – even if unintentionally – to streamline influence operations, as it magnifies certain content and narrows the focus on them.[12]

Another factor that can work in favor of influence operations is the ability of social media users to create and disseminate information and engage

[7] For more on these processes, see Ned Lebow, *Why Nations Fight* (New York: Cambridge University Press, 2010).

[8] Social media includes platforms such as Facebook, WhatsApp, Instagram, LinkedIn, and Twitter.

[9] In 2010, the number of social media users in the world was 0.97 billion, while in 2017 it had already reached 2.62 billion users. See https://bit.ly/2gRTQQk.

[10] Karine Nahon and Jeff Hemsley, *Going Viral* (Cambridge: Polity Press, 2013).

[11] In order to create a browsing experience that matches the worldview of its users, the platform learns the areas of interest and habits of its users, sometimes interfacing with information from other platforms.

[12] Nahon and Rivnai Bahir, "Election Propaganda in the Context of the Internet and Social Media."

in direct, unmediated interactions with others, thus creating an illusion of pluralism, even if the situation is fundamentally different. In influence operations, attackers make use of fake accounts, such as bots or avatars, in order to affect the public agenda and create the impression that public opinion is leaning in a certain direction. The more aware the public becomes of the existence of influence operations on social media, the more critical it will be, thus reducing the effectiveness of these actions.[13]

Cyber Threats of Functional Damage and Cognitive Harm

Although cyber threats that focus on harming functional and cognitive aspects differ from each other, at the same time, both have a number of shared characteristics. Thus, functional damage can cause significant cognitive harm, which, in certain cases, can be greater than the functional damage itself, and therefore can be the main incentive for the attack. For example, a power outage in a large city that lasts a few hours and is discovered by the public to be the result of an intentional attack by an adversary presumably will create panic, fear, uncertainty, and insecurity; that is, the attack will cause much greater cognitive harm than the direct functional damage that occurs due to the lack of electricity for a few hours.

In both threats, the potential circle of people under attack also is increasing. Until recently, cyber campaigns have been characterized as focusing mainly on functional damage to military targets or civilian ones, which constitute the critical infrastructure that enable the society or economy to truly function. Damaging these targets constitutes a severe attack on national security and/or the economic resilience of the side under attack. Meanwhile, in recent years, we have witnessed actions designed to cause functional damage in cyberspace, which is also directed toward social and essential systems and processes, and to a large extent, influence operations are directed toward these systems and processes as well. In other words, the changing battle in cyberspace can be described whereby the entire environment of the side under attack – the physical infrastructure, tangible assets (such as knowledge or secrets), and intangible ones (such as reputation or confidence) – is now the target of the action, whether its objective is functional damage or cognitive influence. In terms of both threats and in the context of attacks on systems

[13] Ibid., p. 4.

that are not essential physical infrastructure, it is difficult to estimate the enormity of the threat and to accurately assess the damage and/or to employ the usual measures of economic damage or loss of human life.

Expanding the circle of people who are attacked points to another shared characteristic of both threats, and that is the tension that arises in a situation in which a democratic regime – based on the principles of freedom of expression, a free press, the right to privacy, and the separation of powers – seeks to defend the main institutions and processes of democracy against these threats described above (functional damage or cognitive influence). In order to ensure that the defense mechanisms against these two threats are not abused, democratic regimes must establish a system of checks and balances to reduce the risks to democracy.

The two threats also have several fundamental differences. They have different objectives (expected achievements), although both threats rely on gathering information, disrupting information, or thwarting information.[14] Damage to information is classified according to three main categories (also known as the CIA model): Confidentiality of Data, Integrity of Data, and Availability of Data. Table 1 shows the differences between functional and cognitive attacks in terms of damage to data.

Offensive cyber actions with a functional objective occur with unauthorized penetration of computerized systems by using hostile code. In addition, unauthorized penetration takes place in order to send a message to an adversary or to gather information. In terms of influence operations, manipulation of the adversary's cognition occurs by transmitting, preventing, or disrupting information, for example, by publicizing false information or leaking confidential information, and can be referred to as using hostile content. These actions are sometimes accompanied by unauthorized penetration of computerized systems, but this is not necessary, and many information or influence operations do not require this.

[14] For the sake of simplicity, here we are presenting the differences between functional damage and cognitive harm to information only, and ignoring cyberattacks against physical systems that are not information systems, such as generators and electrical systems.

Table 1: Classification of Unauthorized Penetrations of Computer Systems

Types of Damage	The Essence of the Action	
	Functional objective	**Cognitive objective**
Damage to the confidentiality of information	Gathering information to produce military/civilian/commercial intelligence	Exposing and publicizing confidential information, for example, leaking or threatening to leak embarrassing information
Damage to the integrity of information	Disrupting and changing data in order to cause physical damage or in order to disrupt the situational awareness	Biasing information and/or planting biased or false information and publicizing it in order to disrupt the situational awareness and sense of reality
Damage to the availability of information	Denial of access to information or disrupting/removing it	Denial of the ability to publicize/disseminate information, for example, blocking platforms where communication and the messages of a political party or candidate are transmitted during an election campaign, in order to prevent the transmission of the messages

Two main types of action make use of hostile content (Table 2). One uses hostile content alone, without malicious penetration of computer systems, for example by leaking information, using avatars in order to place issues on the agenda, slanting the discourse in directions that match the interests of the attacker, inciting terrorism, disseminating rumors, or inciting fear. The other action combines the use of hostile code and hostile content; that is, in order to achieve the objective, unauthorized penetration of information systems occurs, although it is only a means to manipulate the information. Some examples of this include unauthorized penetration of the information systems of polling companies in order to bias the results, thus providing the public with erroneous interpretations of the trends on an issue being polled; stealing information in order to leak it; unauthorized access of mailing lists so that hostile messages can be transmitted; and penetration of mass media systems and/or internet platforms for communicating with the population under attack (website and social media accounts) in order to cause damage, cease activities, disrupt information, and disseminate false information.

Table 2: Influence Using Hostile Code and/or Hostile Content

Damage to computerized infrastructure	**Damage to computerized infrastructure combined with disseminating information**	**Disseminating information in the digital realm; publicizing false information**
• Damage to critical infrastructure • Damage to essential infrastructure • Gathering information in order to carry out operations • "Sending a message" by penetrating systems	• Biasing public opinion polls • Stealing information in order to leak and publicize it • Accessing mailing lists for the purpose of disseminating messages and deception • Penetrating mass media to plant information or disrupt/ damage websites	• Leaking information • Using avatars for social media campaigns • Inciting and encouraging terrorism on the internet • Spreading rumors and inciting fear
Hostile code	**Hostile code and hostile content**	**Hostile content**

Another characteristic that partly distinguishes influence operations from that of cyberattacks causing functional damage relates to the level of secrecy. The effectiveness of influence operations increases to the extent that the malicious actions and the existence of a "guiding hand" behind them are unknown. The cost of exposure in such a case can be high, to the effect of harming the purpose of the entire influence operation. Therefore, covert activities that are under the radar, in the form of a "no-logo" strategy, are almost always preferred. Cyberattacks intended to cause functional damage to computer systems or to disrupt information are also sometimes carried out covertly in order not to reveal the way they were implemented or in order to avoid taking public responsibility. But when these cyberattacks damage the functioning of computer systems, they become a known occurrence.

Conclusion: Implications for Democratic States

In this article, we have focused on the distinction between cyberattacks that aim to damage the functioning of computerized systems, which almost always involve unauthorized penetration of these systems, and influence operations, which do not necessarily make use of unauthorized penetration. It is important to note and understand that this distinction is mainly the product of a cultural-democratic approach that accepts the rules of the game of Western democracies, according to which it is wrong and illegal to penetrate computer systems of others (rooted in conceptions, norms, and legislation). Therefore, this approach sees any action against the functioning of computer systems as an aggressive act that requires defense using various means – legal, police, or military. An output of this democratic approach is the serious concern about intervention in content, narratives, and the media in general given the preference of allowing almost entirely free expression as part of the democratic process. As a result, democratic regimes are quite perplexed regarding the right way to prevent or reduce influence operations and to defend against them, as a result of the concern about government involvement in the media and democratic elections.

Effective defense against cyber influence operations needs to take place vis-à-vis the entire phenomenon of cyberattacks and their threats in the understanding that the attacker does not necessarily distinguish between the two kinds of cyberattacks. As a result, the subjective distinction that exists when looking at this from a democratic perspective poses a serious challenge for the democratic defender: How should a comprehensive, systemic national policy be developed that will consider the various relevant fields for dealing with influence operations and will integrate forces from the various bodies responsible for different aspects of the threats and the responses to them? At the same time, it is necessary to maintain cyberspace as an open space that enables the free flow of knowledge and services and where basic rights are protected, including the rights to freedom of expression and to privacy. These are difficult challenges and dilemmas that democratic states are facing. Non-democratic states, which do not address these issues, find it easier to formulate a systemic defense concept that does not distinguish between actions with a functional objective and those aimed at a cognitive-related objective, either at the conceptual, organizational, or operational levels.

Based on these insights, we believe that from the democratic perspective, a central part of addressing the challenge posed by the phenomenon of cyber influence operations is identifying and mapping all the parties whose involvement is necessary for obtaining effective defense, as well as the interfaces between them. This includes intelligence for identification, prevention, and deterrence; cyber technology for countering actions comprised of unauthorized penetration of computer systems; legislation and enforcement for coping with incitement and the dissemination of hostile content; public diplomacy for neutralizing the influence of hostile content and for raising awareness; and education for a critical perspective toward content on the internet. It is also worth examining the possibility of utilizing existing knowledge and capabilities in academia and in the private market to this end.

The question of the role of national cyber security agencies in addressing cyber influence operations needs to be asked. In other words, in addition to their responsibility of defending the national or civilian cyberspace against attacks that penetrate computer systems, why not give them the responsibility for defending against cognitive operations? They are seemingly the natural agencies for these activities, since, as emphasized above, attackers do not usually distinguish between penetrating computer systems – an area that cyber security agencies are responsible for defending against – and influence operations. If so, why not expand the responsibility of these defense agencies to include this natural task?

In our view, the answer lies in two fundamental reasons relating to the nature of these security organizations. Firstly, in many countries, the cyber defense agencies are part of the military or the police. Giving them responsibility for defending against hostile content – and not just hostile penetration – contradicts the balances that exist in democratic regimes. It would thus be a mistake to assign them with this responsibility of probing media organizations, taking an interest in their content, and making decisions about it. Secondly, even in countries where cyber defense agencies are not part of the military or the police, such as the Israel National Cyber Directorate, there is a good reason not to connect these two. In countries characterized as democratic, these organizations require that the civilian sectors place great trust in them; only a high level of trust between a government agency and private organizations will enable government security agency to access information, analyze it from a national perspective, and work with the private organizations on their "turf." This trust is a fundamental component of the ability of government security agencies to defend civilian cyberspace. Without it, regardless of the powers the defense agency has, it will not be able to fulfill this responsibility. Achieving such trust is based, first and foremost, on cyber security agencies having a disinterest in content and showing concern only in defending against the penetration of computerized systems. This trust could be severely undermined if security agencies take positions and make decisions regarding content.

These reasons and explanations lead to the conclusion that existing cyber security agencies should not be tasked with handling the defense against influence operations. Nonetheless, cyber security agencies must not be excluded from the overall national system-wide effort to cope with the threat of such operations.

The tension between the need to defend against influence operations and the need and obligation to maintain basic civil rights highlights the importance of the public discussion on the question of "what are the rules of the game," or in other words, what is prohibited influence and which tools and methods are illegitimate. Thus, an effort should be made to expand the discussion on the issues that will help define the boundaries of legitimacy of influence activities. This includes (but is not limited to):

a. Defining boundaries of the legitimacy of activities aimed at the masses, which seek to create cognitive influence, for example, activities through networks of bots.[15]
b. Defining boundaries of the legitimacy in harming essential and important bodies and processes to society and the state through actions in cyberspace.
c. Defining boundaries regarding the legitimacy of the involvement of defense agencies against actions that combine hostile code and content, including the ability to contend with situations of unauthorized penetration of computerized information systems in essential and important bodies or processes of the state and society. An example is dealing with the abuse of unclassified information attained by unauthorized penetration of computerized information systems.
d. Examining the possibility of developing national and international mechanisms that provide a framework for action and define the responsibility of the companies operating social networks, in the face of threats.[16] This should relate to the architecture of gathering information on users, the flow and filtering of information to them, and the virality in transmitting messages.

Another important issue for effectively coping with influence operations relates to the public's confidence in state institutions. Influence operations

[15] For example, in an article published in the *New York Times* on July 15, 2017, under the headline "Please Prove You're not a Robot," researcher Tim Wu from Columbia University suggested defining botnets as "enemies of humanity," similar to pirates.

[16] Tim Wu argued in his opinion piece that in the absence of an economic incentive for companies operating social networks, it is difficult to cope with the problem of botnets.

aim in part to harm social stability and undermine public confidence in state institutions and systems. Thus, a high level of public confidence in the party against which hostile content is used is essential to be able to cope with an influence operation effectively.[17] We must invest in finding ways to strengthen and consolidate trust between the public and the various state institutions. From the perspective of the cyber defense organization, one way is to cultivate a continuous and direct connection with the public and to promise that in times of crisis the reliability of computerized systems and their information will be quickly verified, and this will be shared with the public.[18]

In conclusion, the phenomenon of influence operations has become a common pattern of action and significantly threatens the ability of states to make decisions independently. Defense preparations as part of the cyber campaign have so far focused mainly on defending against functional damage. The intensified use of influence operations requires that the unique characteristics of this type of activity is addressed, while ensuring the openness and freedom of cyberspace and the upholding of basic civil rights.

[17] For example, Ron Schleifer argues that "an effective medium that Hamas used in Operation Cast Lead was spreading rumors. Among others, it spread rumors regarding the number of IDF casualties, but since the IDF Spokesperson enjoys a high level of credibility, these false rumors did not cause damage." See Schleifer, "Psychological Warfare in Operation Cast Lead," p. 22.

[18] Rand Waltzman, "The Weaponization of Information – The Need for Cognitive Security," Testimony presented before the Senate Armed Services Committee, Subcommittee on Cybersecurity, Rand Corporation, April 27, 2017, p. 6.